CYBERSECURITY

Strategies Emerging to Fill in the Physical Security Gaps with Zero Trust

The U.S. cyber and security industry has made great strides after a long-standing lag by the federal government toward centralized Zero Trust efforts.

Patrick Miller, Steven Brown, Thomas Segars, Edward M. Levy

Note -- STE/SIW Exclusive Special Content: Over the next several issues of STE, we will present a four-part series of articles on bringing Zero Trust Architecture (ZTA) to the edge (how and why) with a holistic mitigation approach to increasing threat response, safety, and overall mission success.

As 2025 quickly approaches, and with 2024's major technology industry trade shows winding down, it is clear that the tech industry has made significant cyber advances in various niche applications. Most readers will recall that it has not always been that way. Through the outcry of the cyber industry, after the federal government's perceived feet-dragging on unifying Zero Trust efforts helped create a decade-long environment ripe for cyber exploitation, new legislation has paved the way to secure the tech industry better. However, between the rather slow progression of policy and the speed of technological advancements, a gap now highlights elusive questions surrounding technology peripherals and the associated

components leading back to the head-end and video assessment center: is physical security equipment critical, and where's the edge?

Authenticated and Verified Overwatch – Outsiders/Insiders:

In military operations, cyber or information operations are largely regarded as the fifth dimension of warfare. For the billions of dollars spent across the U.S. protecting data from outsiders, when compared to the number of successful cyber breaches, and not at all discounting the number of attempts, the rhetorical question remains rather obvious as characterized by the author through the lens of American football: is the U.S. tech industry in a perpetual state of defense, something akin to continuous blocking and tackling with episodic injuries…or in an offensive posture where the U.S. industry keeps the opponent inferior and at bay by throwing completed passes and scoring touchdowns?

Adding another complexity, how is the game impacted when, say, a referee is biased against a team and actively works to influence a particular outcome? Perhaps not in football, but in the real world, the threat is real. Gone are the days when companies focused mainly on outside actors to protect Information Technology (IT) and Operational Technology (OT) systems along with sensitive data and capabilities. In today's globally connected environment, coupled with a rather lukewarm economy and ubiquitous life stressors, many companies are keenly aware of the need to also focus inside the

organization to combat the insider threat posed by wayward, disgruntled, and ill-intended employees. The two threats, insiders and outsiders, are inextricably linked by their desire to exploit, destroy or disrupt a company's mission--or sometimes just for personal gain. Either threat can be crippling in its own right, but together they pose an ominous danger. Regardless of the scenario or the threat actors, the organization remains continuously on guard and is, as a result, forced to embrace a position of zero trust and burden all associated risks and costs for achieving higher levels of authentication and verification.

Zero Trust

John Kindervag coined the term Zero Trust in 2010, which is now codified in the National Institute of Standards and Technology (NIST) Special Publication 800-207. The concept is largely centered around seven foundational tenets. In its most basic form, Zero Trust refers to the framework that no one can be trusted and everything must be verified.

Yet Zero Trust on its own is simply not enough. To be even more effective, Zero Trust must be complemented with comprehensive policies, which are also enacted and enforced and bind *all* users to the same prescribed rules. Any hint of daylight between policy and Zero Trust efforts could prove catastrophic, a concern exacerbated by the long-standing Achilles Heel of that inconvenient point where physical security and cybersecurity converge--to many U.S. customers, *convenience* is the only goal. As tech companies continue

efforts at revolutionizing their security efforts, either begrudgingly or for the least amount of financial investment possible, one example of capitalizing on this Zero Trust concept is to push the technology beyond the user edge and into the sensor edge—where extending Zero Trust to the sensor's edge underscores the importance of thinking outside the box and staying ahead of adversarial cyberspace infiltration attempts by moving authentication *to the scene itself*.

Where's The "Real" Edge?:

Thanks largely to the 2020 coronavirus epidemic, telework and wider applications of "work-on-the-go" have perhaps redefined the "user edge," allowing users access to critical files and company data lakes from an employee's personal devices.

Similarly, one company has been focusing on redefining the edge of sensors and video assessments in high-end security applications. Under Zero Trust's tenets - trust no one and verify everything - after eight years of research and development Prometheus Security Group, in Austin, Texas was by all accounts the first company to bring Zero Trust Architecture (ZTA) to a new edge, pushing patented technology to the sensor, reader and camera edges, also known as physical security equipment (PSE). In an industry first, PSG's patented solution encrypts and secures the data between the head-end and the equipment edge, a revolutionary concept PSG dubs "scene authentication" and one that redefines previous limits of the edge.

> *Zero Trust on its own is simply not enough. To be even more effective, Zero Trust must be complemented with comprehensive policies, which are also enacted and enforced and bind all users to the same prescribed rules.*

Significant blemishes in U.S. history, such as the 2014 cyber infiltration of Sony Pictures and the 2016 cyberattack on the Democratic National Convention information systems, serve as stark reminders about nation-state actors' advanced capabilities to reach out and touch even U.S. companies and infrastructure beyond the IT closets and keyboards. A more recent example is the almost 3-year conflict between Russia and Ukraine. At the conflict's onset in 2022, Russia used cyberattacks to soften targets and sow chaos across the country, and to dismantle Ukraine's command, control, and communications capabilities ahead of the ground invasion. Though some scholars assert that the conflict's cyber operations fall squarely in the support realm as opposed to having decisive or crippling effects on the outcome, attack strategies for IT and OT systems are

only limited by the imagination and, therefore, demand continuous exploration of the edge. Would anyone have predicted the edge moving into the physical security equipment space 10 years ago?

Continuous edge evaluation is paramount for the U.S. industrial base to remain secure. Modern technology efforts must demand every piece of distributed and employed technology be analyzed, protected, encrypted, and *trusted*, with redundant protections, so administrators and operators of the technology can all but guarantee the safety and security of data--and in sensitive government spaces and strategic locations, mission accomplishment without compromising the team's safety.

A natural byproduct of redefining the edge is increased confidence in mitigating an insider threat. However, administrators and security professionals are cautioned not to overlook or discount any insider threat potential risk indicators employees might display. Something as "simple" as pushing Zero Trust to the sensor edge does, however, provide confidence that assuming all Zero Trust principles and tenets are also aligned (i.e., users authorized, devices authenticated, etc.), the actual scene being displayed in a video management system is encrypted, secured, and factual. In other words, the scene visually presented on a monitor in an operations center is reliable and trustworthy--as if a security response team was physically present at the scene and seeing it for themselves. Today, armed security teams must be deployed to an alarm in some federal government spaces even though immediate visual assessment of the site can be made from a remote location. The power of moving the

edge into scene authentication resolves manpower deficits, eliminates threats of spoofing, mitigates time/distance factors between affected sites and the location of alarm response teams, and has the potential to save money in the long run.

Is Moving the Edge Important?:

In a word, yes. Today's geopolitical landscape and the U.S.'s status as a world superpower demand continued technological advancements and security efforts for the DIB. Suppose the U.S. is, in fact, one step behind global cyber criminals, regardless of the actor's intent. In that case, the ramifications of the U.S. not moving to first place ahead of would-be cyber actors could prove debilitating and unsustainable for the U.S. The great Chinese General Sun Tzu would succinctly tell us, "If quick, I survive. If not quick, I am lost. This is death."

Cybercriminals often find voids, exploring vulnerabilities and loopholes in the U.S. government's push toward Zero Trust. Security practitioners should not be lulled into a false sense of security or rest on the laurels of Zero Trust alone--there is much work to be done. Some of that work includes continued evaluation of the edge and its relationship to IT and OT components. Security advancements can appear quite different between the federal government and the corporate world, where slow advancements in technological defenses could mean continued survival ... or certain death. In the corporate world, executives neglecting the relationship between cyber and physical security may result in unintentional

gaps between the two disciplines. Cyber is the newest player and far more sexy than physical security. Yet, physical security voids can just as easily put corporations in a position of unenviable *reputational risk*, opening a chasm for the company through lost revenue, remediation costs, lawsuits, or worse.

On the federal side, the risks are unimaginable. Two military Service components – the United States Air Force and the United States Navy – are directly responsible for the safekeeping of strategic weapons in all 3 legs of the nuclear triad. Allowing an adversary to infiltrate U.S. cyber and PSE mechanisms could, on the one hand, simply compromise a particular capability. On the other hand, an infiltration could altogether remove, as a response option, the President of the United States' ability to employ the weapons wherever and whenever needed--to include in the nation's defense. In the eyes of many foreign powers, the U.S. is a lucrative target and the public does not have all the information.

The Waterfall report is informative and chock-full of important data for the industry to analyze. Yet one key notation refers to the cyberattacks "in the public record," The importance of this notation should not be lost on the reader, which subtly tells us federal government systems, including classified systems and sensitive operations directly tied to national security, are cloaked in secrecy and therefore not reported in these unclassified publications. Yet, one can assume these classified IT and OT systems are also targeted by cybercriminals, hacktivists, and nation-states alike.

Many federal government attacks, if not all, are held close to the government's chest--for good reason. Imagine a future where hacktivists and nation-state actors successfully limit the United States' ability to leverage any of the instruments of power (diplomacy, information, military or economic), especially if those attacks can be executed without any kinetic activity. If the U.S.'s national security is at risk, or even in question, how can it remain a world superpower and adequately posture for a potential future fight? Just one incident in the United States where a nation-state actor gains access to federal OT systems in a strategic weapons area could prove detrimental to U.S. missions at home and abroad. At the very least, it will degrade the U.S.'s global strategic posture.

The Zero Trust journey is fraught with challenges. It is undoubtedly expensive, but moving the edge from server rooms and beyond the camera lens also strengthens the cybersecurity posture necessary to preserve critical infrastructure, critical assets, and strategic capabilities which may very well define future U.S. survival (or global influence at the very least). Even the Department of Defense (DoD), with its intricate web of mission partners in a wide variety of global settings and environments, including the DIB, is constantly navigating enterprise checks and balances, where the result is the ability to allow authorized users authenticated access to DoD information systems from wherever they are, yet do so while keeping the IT and OT systems secure.

Moving the edge has important intangible benefits, too. In an acknowledgment to account for insider threats, the Department of

Defense's Zero Trust Strategy highlights four Strategic Principles tied to four categories: of Mission-Oriented, Organizational, Governance, and Technical, the latter of which contains a sub-category, *Scrutinize and Analyze Behavior*, to wit, "All events within our IE must be continuously monitored, collected, stored, and analyzed based on risk profiles and generated in near-real time for both user and device behaviors." The Department's clear linkage of counter-insider threat principles to Zero Trust activities is revolutionary. It strengthens the U.S. industrial base and protects its critical systems and infrastructure.

Encryption Solutions

Five key considerations for tackling Zero Trust

Mark Cassetta

Cybersecurity

How embracing Zero Trust can be transformative

Jaye Tillson

Information Security

The Zero Trust journey

Bhagwat Swaroop

Conclusion:

The U.S. cyber and security industry has made great strides after a long-standing lag by the federal government toward centralized Zero Trust efforts, so much so that cyber and security companies are constantly pushing the limits of defining the edge. Since being codified in Executive Order 14028 just three short years ago, Zero

Trust is very much something akin to a north star for cybersecurity practitioners, and the U.S. industrial base is in a full-court press toward implementation. Fortunately, the linkage of Executive Order 13587 for insider threat with Executive Order 14028 only strengthens the collective security efforts. It helps protect the NIB from nefarious actors inside and outside the organization. Perhaps not as obvious, these advancements also serve as a reminder that physical security equipment plays a pivotal role in security IT and OT systems and should not be overlooked.

As Zero Trust continues to evolve and the limits of the edge are moved, here are another couple of questions for the reader to ponder: Will the evolution of AI complement or detriment physical security equipment, especially in areas housing our nation's most strategic assets? And what is the nexus between AI and Zero Trust and the response mission engagement?

S-